where

$$w_i = \prod_{j \neq i} p_j, \text{and} \dots$$

On page 12, lines 10 through 12, replace

"*$M = M_1 (W_1^{-1} \bmod p_1)\, w_1 \bmod n + M_2 (W_2^{-1} \bmod p_2)\, W_2 \bmod n$*

$+ M_3 (W_3^{-1} \bmod p_3)\, W_3 \bmod n$

where

$W_1 = p_2 p_3$, $W_2 = p_1 p_3$, and $W_3 = p_1 p_2$."

with

$$M \equiv M_1 (w_1^{-1} \bmod p_1)\, w_1 \bmod n + M_2 (w_2^{-1} \bmod p_2)\, w_2 \bmod n + M_3 (w_3^{-1} \bmod p_3)\, w_3 \bmod n$$

where

$w_1 = p_2 p_3$, $w_2 = p_1 p_3$, and $w_3 = p_1 p_2$.

In The Claims:

14. (Once Amended) A method for establishing cryptographic communications comprising the step of:

encoding a plaintext message word M to a ciphertext word [signal] C, where M corresponds to a number representative of a message and

$0 \leq M \leq n-1$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and where the ciphertext word C is a number representative of an encoded form of message word M, [wherein] said encoding step [comprises] including the [step] steps of[:],

[transforming said message word signal M to said ciphertext word signal C whereby

$$C_1 = M_1^{e_1} \bmod p_1,$$
$$C_2 = M_2^{e_2} \bmod p_2,$$
$$\vdots$$
$$C_n = M_n^{e_n} \bmod p_n,$$

$$M_1 = M \pmod{p_1},$$
$$M_2 = M \pmod{p_2},$$
$$\vdots$$

$M_n = M \pmod{p_n}$,

$e_1 = e \bmod (p_1 - 1)$,
$e_2 = e \bmod (p_2 - 1)$,
⋮
$e_n = e \bmod (p_n - 1)]$

defining a plurality of k sub-tasks in accordance with,

$C_1 \equiv M_1^{e_1} \pmod{p_1}$,

$C_2 \equiv M_2^{e_2} \pmod{p_2}$,

⋮

$C_k \equiv M_k^{e_k} \pmod{p_k}$,

where

$M_1 \equiv M \pmod{p_1}$,
$M_2 \equiv M \pmod{p_2}$,
⋮
$M_k \equiv M \pmod{p_k}$,

$e_1 \equiv e \pmod{(p_1 - 1)}$,
$e_2 \equiv e \pmod{(p_2 - 1)}$, and
⋮
$e_k \equiv e \pmod{(p_k - 1)}$,

where e is a number relatively prime to (p_1-1), (p_2-1) , …, and (p_k-1),

solving said subtasks to determine results $C_1, C_2 \ldots C_k$,

combining said results of said subtasks in accordance with a recursive combining process to produce said ciphertext word signal C whereby,

Y_i [=] $\equiv Y_{i-1} + [([M_i]C_i - Y_{i-1})\ ([W]w_i^{-1} \bmod p_i) \bmod p_i] \bullet [W]w_i \bmod n$

[for $i \geq 2$] $2 \leq i \leq k$, and

$[C = Y_k, Y_1 = M_1, \text{and } W_i = \prod_{j<i} p_j.]$

$C = Y_k, Y_1 = C_1, \text{and } w_i = \prod_{j<i} p_j.$

---

15. (Once Amended) A method [according to claim 1] for establishing cryptographic communications, comprising the [further step] steps of:

decoding [the] a ciphertext word [signal] C to [the] a message word [signal] M, wherein M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, $p_1, p_2, \ldots, p_k$ are distinct prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

[wherein] said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decoding step [comprises] including the [step] steps of[:],

[transforming said ciphertext word signal C, whereby:]

(i) defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} \pmod{p_1},$$
$$M_2 \equiv C_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv C_k^{d_k} \pmod{p_k},$$

where

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

(ii) solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

(iii) combining said results of said subtasks in accordance with a recursive combining process to produce said message word M in accordance with,

$$Y_i [=] \equiv Y_{i-1} + [(M_i - Y_{i-1})([W]w_i^{-1} \bmod p_i) \bmod p_i] \cdot [W]w_i \bmod n$$

where [$i \geq 1$] $2 \leq i \leq k$, and

$$[M = Y_k, Y_1 = C_1, \text{and } W_i = \prod_{j<i} p_j.]$$

$$M = Y_k, Y_1 = M_1, \text{and } w_i = \prod_{j<i} p_j.$$

---

16. (Once Amended) A cyptographic communications system comprising:

a communication medium;

an encoding means coupled to said communication medium and adapted for transforming a transmit message word [signal] M to a ciphertext word [signal] C and for transmitting said ciphertext word C on said [channel] medium, where M corresponds to a number representative of a message, and

$0 \leq M \leq n\text{-}1$ where n is a composite number of the form

$n = p_1 \bullet p_2 \bullet \ldots \bullet p_k$,

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and where C corresponds to a number representative of an enciphered form of said message, and corresponds to

$[C \equiv M^e \bmod (n)]$

$C \equiv M^e \pmod n$,

where e is a number relatively prime to [$\text{lcm}(p_1\text{-}1, p_2\text{-}1, \ldots, p_k\text{-}1)$] $(p_1\text{-}1), (p_2\text{-}1), \ldots,$ and $(p_k\text{-}1)$; and

a decoding means coupled to said communication medium and adapted for receiving C [from said channel] via said medium and for transforming C to a receive message word [signal] M' where M' corresponds to a number representative of a deciphered form of C [and corresponds to] ,said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1\text{-}1)(p_2\text{-}1) \ldots (p_k\text{-}1)),$$

said decryption process including the steps of

(i) defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$

$C_k \equiv C \pmod{p_k}$,

where,

$d_1 \equiv d \pmod{(p_1 - 1)}$,
$d_2 \equiv d \pmod{(p_2 - 1)}$,

$d_k \equiv d \pmod{(p_k - 1)}$,

$M_1' \equiv C_1^{d_1} \pmod{p_1}$,
$M_2' \equiv C_2^{d_2} \pmod{p_2}$, and

$M_k' \equiv C_k^{d_k} \pmod{p_k}$,

(ii) solving said sub-tasks to determine results M_1', M_2', ... M_k', and

(iii) combining said results of said subtasks by a recursive combining process to produce said receive message word M' in accordance with

$Y_i [=] \equiv Y_{i-1} + [([M_i/] M_i' - Y_{i-1}) ([W]w_i^{-1} \bmod p_i) \bmod p_i] \bullet [W]w_i \bmod n$

where $[i \geq 1]$ $2 \leq i \leq k$ and

$[M' = Y_k, Y_1 = C_1, \text{and } W_i = \prod_{j<i} p_j.]$

$M' = Y_k, Y_1 = M_1, \text{and } w_i = \prod_{j<i} p_j,$

whereby M'=M.

17. (New) A method for establishing cryptographic communications comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$,

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2, p_1, p_2, ..., p_k are distinct prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

18. (New) A method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word M'.

19. (New) A method as recited in claim 18 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i'-Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \le i \le k$, and

$$M' = Y_k,\ Y_1 = M_1',\ \text{and}\ w_i = \prod_{j<i} p_j.$$

20. (New) A method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word M'.

21. (New) A method as recited in claim 20 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

22. (New) A cyptographic communications system comprising:

a communication medium;

an encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

wherein k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message and corresponds to

$C \equiv M^e \pmod{n}$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

a decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)},$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M' whereby M'=M.

23. (New) A cyptographic communications system as recited in claim 22 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word M'.

24. (New) A cyptographic communications system as recited in claim 23 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k,\ Y_1 = M_1,\ \text{and}\ w_i = \prod_{j<i} p_j.$$

25. (New) A cyptographic communications system as recited in claim 22 wherein said decoding means is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

26. (New) A cyptographic communications system as recited in claim 25 wherein said decoding means is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

27. (New) A method for establishing cryptographic communications comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2, $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$
$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, $C_{2, \ldots}$ C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

28. (New) A method as recited in claim 27 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said ciphertext word C.

29. (New) A method as recited in claim 28 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k,\ Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j.$$

30. (New) A method as recited in claim 27 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said ciphertext word C.

31. (New) A method as recited in claim 30 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

32. (New) A cyptographic communications system comprising:

a communication medium;

an encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2, $p_1, p_2, \ldots, p_k$, are distinct prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$
$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1) , …, and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

33. (New) A cyptographic communications system as recited in claim 32 wherein said encoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said ciphertext word C.

34. (New) A cyptographic communications system as recited in claim 33 wherein said encoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k, Y_1 = C_1, \text{and } w_i = \prod_{j<i} p_j.$$

35. (New) A cyptographic communications system as recited in claim 32 wherein said encoding means is operative to combine said results of said sub-tasks by performing a summation process to produce said message word C.

36. (New) A cyptographic communications system as recited in claim 35 wherein said encoding means is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where,

$$w_i = \prod_{j \neq i} p_j.$$

37. (New) A method for establishing cryptographic communications, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n\text{-}1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, p_1, p_2, ..., p_k are distinct prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e \pmod n$,

and wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$;

said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1\text{-}1)(p_2\text{-}1) \ldots (p_k\text{-}1))$,

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$M_1 \equiv C_1^{d_1} \pmod{p_1}$,

$M_2 \equiv C_2^{d_2} \pmod{p_2}$,

$\vdots$

$M_k \equiv C_k^{d_k} \pmod{p_k}$,

wherein

$C_1 \equiv C \pmod{p_1}$,
$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,
$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$\vdots$

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

combining said results of said sub-tasks to produce said message word M.

38. (New) A method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said message word M.

39. (New) A method as recited in claim 38 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M = Y_k, Y_1 = M_1, \text{and } w_i = \prod_{j<i} p_j.$$

40. (New) A method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said message word M.

41. (New) A method as recited in claim 40 wherein said summation process is performed in accordance with

$$M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

42. (New) A cyptographic communications system comprising:

a communication medium;

a decoding means communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, p_1, p_2, ..., p_k are distinct prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$M_1' \equiv C_1^{d_1} \pmod{p_1}$,
$M_2' \equiv C_2^{d_2} \pmod{p_2}$,
$\vdots$
$M_k' \equiv C_k^{d_k} \pmod{p_k}$,

wherein,

$C_1 \equiv C \pmod{p_1}$,
$C_2 \equiv C \pmod{p_2}$,
$\vdots$
$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,
$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

43. (New) A cyptographic communications system as recited in claim 42 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word M'.

44. (New) A cyptographic communications system as recited in claim 41 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M = Y_k,\ Y_1 = M_1',\ \text{and}\ w_i = \prod_{j<i} p_j.$$

45. (New) A cyptographic communications system as recited in claim 42 wherein said decoding means is operative to combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

46. (New) A cyptographic communications system as recited in claim 45 wherein said decoding means is operative to perform said summation process in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

47. (New) A method for generating a digital signature comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, wherein k is an integer greater than 2, $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d \pmod{n}$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

48. (New) A method as recited in claim 47 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said ciphertext word C.

49. (New) A method as recited in claim 48 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k,\ Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j.$$

50. (New) A method as recited in claim 47 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said signed ciphertext word C.

51. (New) A method as recited in claim 50 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

52. (New) A digital signature generation system comprising:

a communication medium;

a digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ wherein k is an integer greater than 2, $p_1, p_2, \ldots, p_k$, are distinct prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d \pmod n,$$

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$$d \equiv e^{-1} \bmod ((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1) , …, and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said signed ciphertext word C.

53. (New) A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said signed ciphertext word C.

54. (New) A digital signature generation system as recited in claim 53 wherein said digital signature generating means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k, Y_1 = C_1, \text{and } w_i = \prod_{j<i} p_j.$$

55. (New) A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a summation process to produce said signed message word C.

56. (New) A digital signature system as recited in claim 55 wherein said signature generating means is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

57. (New) A digital signature process comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, p_1, p_2, ..., p_k are distinct prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$C \equiv M^d \pmod n$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1) , ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$M_2' \equiv C_2^{e_2} \pmod{p_2}$,

$\vdots$

$M_k' \equiv C_k^{e_k} \pmod{p_k}$,

wherein

$C_1 \equiv C \pmod{p_1}$,
$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$e_1 \equiv e \pmod{(p_1 - 1)}$,
$e_2 \equiv e \pmod{(p_2 - 1)}$, and

$\vdots$

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

58. (New) A digital signature process as recited in claim 57 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word M'.

59. (New) A digital signature process as recited in claim 58 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k,\ Y_1 = M_1',\ \text{and}\ w_i = \prod_{j<i} p_j.$$

60. (New) A digital signature process as recited in claim 58 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word M'.

61. A digital signature process as recited in claim 60 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

62. (New) A digital signature system comprising:

a communication medium;

a digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form

$n = p_1 \bullet p_2 \bullet \ldots \bullet p_k$,

wherein k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

a digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$
$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$
$$\vdots$$
$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$e_1 \equiv e \pmod{(p_1 - 1)}$,
$e_2 \equiv e \pmod{(p_2 - 1)}$,

$\vdots$

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M'

whereby M'=M.

63. (New) A digital signature system as recited in claim 62 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word M'.

64. (New) A digital signature system as recited in claim 63 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$M' = Y_k$, $Y_1 = M_1'$, and $w_i = \prod_{j<i} p_j$.

65. (New) A digital signature system as recited in claim 62 wherein said decoding means is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

66. (New) A digital signature system as recited in claim 65 wherein said decoding means is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$w_i = \prod_{j \neq i} p_j$.